NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Oil executive pleads not guilty to charges. An oil executive pleaded not guilty November 26 at the Stark County, North Dakota Courthouse to a felony charge that he threatened area drinking water with his company's hydraulic fracturing, or "fracking," wastewater disposal practices. Earlier this year, the North Dakota Attorney General's Office charged the suspect with a Class C felony, arguing that a company led by him knowingly attempted to deceive Industrial Commission inspectors. The State has alleged that the suspect, president of Executive Drilling LLC at the time of the alleged crime, directed employees of another company to modify their fracking wastewater disposal practices, which are watched closely because of environmental concerns. He directed the injection of salt water used in the fracking process into a well that was not properly insulated from groundwater near the Lodgepole formation in Stark County, according to court documents. It is unknown at this time if drinking water was contaminated from the alleged negligence and any findings related to groundwater testing would not be released until a trial, according to the North Dakota Department of Mineral Resources.
Source: http://www.thedickinsonpress.com/event/article/id/63338/

Regional

(Minnesota) **Two wanted in Fergus Falls mail, identity thefts.** The Detroit Lakes Tribune reported November 28 that, according to a WDAY 6 Fargo news report, law enforcement in Fergus Falls, Minnesota, were looking for two people in connection to stealing mail and using it for identity theft. Police said the two suspects took blank checks and other mail from at least six homes. The two took the checks from credit card mailings and use them to deposit money into their own accounts at Affinity Plus Credit Union. The two then allegedly worked their way down Interstate 94, writing more false checks and stealing more mail in the Anoka area, police said. Police believed the two were somewhere in Wisconsin, passing counterfeit bills. One of the suspects pleaded guilty to 35 counts of mail theft in Becker County in 2006. Source: http://www.dl-online.com/event/article/id/71474/group/homepage/

National

Nothing Significant to Report

International

South Korea finds more nuclear parts with fake documents. South Korean nuclear regulators have discovered nearly a thousand more parts supplied for nuclear power plants with fake quality certificates, they said November 28, adding that this would not lead to further reactor shutdowns. Revelations that fake certificates were supplied by eight firms forced the shutdown of two of the country's 23 reactors in November, raising the risk of winter power shortages. A third reactor was subjected to an extended maintenance period after microscopic cracks were found in tunnels that guide control rods. Nuclear normally accounts for a third of South Korea's

power supplies. The Nuclear Safety and Security Commission said further investigation had uncovered 919 parts of 53 items supplied by two new firms with forged quality documents. Most had been fitted in six reactors — five of which were already affected by the earlier revelations. The country's sole power transmitter and distributor, Korea Electric Power Corp, said it would hold a drill November 28 to check for stable power supply and gauge the chances of outages this winter.
Source: http://www.nucpros.com/content/south-korea-finds-more-nuclear-parts-fakedocuments

Banking and Finance Industry

Unencrypted payment data on business networks at 70 percent. SecurityMetrics published its second annual Payment Card Threat Report revealing unencrypted Primary Account Number (PAN) storage remains alarmingly high. Virtually no change occurred between 2011 and 2012, with card data storage on corporate systems declining less than one quarter of a percent. The study exposed that greater than 10% of merchants store magnetic stripe track data, essential for the illegal reproduction of credit and debit cards. Financial, hospitality, and retail industries accounted for 55 percent of the total unencrypted payment card data storage among businesses tested. Businesses that store unencrypted payment card data directly violate Payment Card Industry Data Security Standard (PCI DSS) requirements and are more likely to be exploited and suffer severe financial repercussions. Source: http://www.net-security.org/secworld.php?id=14034&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

Chemical and Hazardous Materials Sector

U.N. atom agency says stolen information on hacker site. The U.N. nuclear watchdog said information stolen from one of its former servers had been posted on a hacker Web site November 27, and it was taking "all possible steps" to ensure its computer systems and data were protected. The stolen information was contained in a statement by a hacking group. The International Atomic Energy Agency (IAEA) said the theft concerned "some contact details related to experts working" with the Vienna-based agency but it did not say who might have been behind the action. A Western diplomat said the stolen data was not believed to include information related to confidential work carried out by the IAEA. The statement posted under the name "Parastoo" included a large number of email addresses. An IAEA spokeswoman said the agency "deeply regrets this publication of information stolen from an old server that was shut down some time ago". "The IAEA's technical and security teams are continuing to analyze the situation and do everything possible to help ensure that no further information is vulnerable," she said. Source: http://www.reuters.com/article/2012/11/27/net-us-nuclear-iaea-hackingidUSBRE8AQ0ZY20121127

Commercial Facilities

Nothing Significant to Report

Communications Sector

Nothing Significant to Report

Critical Manufacturing

NHTSA recall notice - Mitsubishi Fuso FE and FG series fuel pipes. Mitsubishi Fuso Truck of America (MFTA) announced November 30 the recall of 13,644 model year 2005-2007 FE83D, FE84D, FE85D, and FG84D trucks manufactured from May 27, 2004 through May 14, 2007. The fuel pipes may crack due to an improper manufacturing process. Additionally, the fuel pipe flare nuts may have been insufficiently tightened. Cracked fuel pipes or loose fuel pipe flare nuts may leak fuel. A fuel leak in the presence of an ignition source may result in a vehicle fire. MFTA will notify owners, and dealers will inspect the fuel pipes and tighten or replace them as needed. Source: http://wwwodi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rclD=12V545000&summary=true&prod_id=202368&PrintVersion=YES

Harbor Freight Tools recalls cordless drill due to fire and burn hazard. The U.S. Consumer Product Safety Commission, in cooperation with Harbor Freight Tools, November 27 announced a voluntary recall of about 108,000 cordless drills. The black trigger switch on the 19.2v cordless drill can overheat, posing a fire and burn hazard to consumers. Harbor Freight Tools has received one report of a drill overheating and burning through the handle of the unit, which resulted in a consumer receiving a minor injury. The drills were sold at Harbor Freight Tools stores nationwide, via catalog and online, from April, 2008 through May 2012. Consumers should stop using the recalled drill immediately, remove the rechargeable battery, and contact Harbor Freight Tools to receive a free replacement drill. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml13/13047.html

Defense/ Industry Base Sector

U.S. body armor plates being replaced. The U.S. military said it would issue replacement body armor plates to troops in the field after the manufacturer issued a recall, UPI reported November 25. Thousands of armor plates used in body armor issued to U.S. Special Operations personnel were recalled after defects were detected in about 5 percent of them, Special Operations Command told ABCNews.com. The defects were found in the Generation III armor plates manufactured by California's Ceradyne, Inc. Ceradyne has been replacing the plates with the Generation II model. The plates are inserted into standard bullet proof vests as an added measure of protection. Special Operations Command said there were no casualties linked to Generation III plates. Source: http://www.upi.com/Top_News/US/2012/11/25/US-body-armor-plates-being-replaced/UPI-23791353861715/#axzz2DLFMsr9V

Emergency Services

(New York) **Shredded police documents showered down on Macy's parade spectators.** Two individuals watching the Macy's Thanksgiving Day Parade in New York City November 22 discovered that shredded documents containing sensitive police information were among the confetti being thrown for the parade. After picking it up and examining it, they realized it contained numbers and the acronym "SSN." They thought the number was likely a social security number, and decided to gather more of the confetti strips laying around. They realized that some contained entire phone numbers, addresses, more social security numbers, license plate numbers, and other confidential information. Some contained information regarding police incident reports and police controlled events. The logo and the information on the shredded documents made it possible to tie them to the Nassau County Police Department, which polices parts of Long Island. It was unknown how the strips ended up at the parade, but after being notified of the matter, the Nassau County Police Department stated that they will be conducting an investigation into this matter as well as reviewing their procedures for the disposing of sensitive documents. Macy's said that they used only commercially manufactured multicolor confetti for the parade. Source: http://www.net-security.org/secworld.php?id=14012

Energy

Nothing Significant to Report

Food and Agriculture

FDA suspends peanut butter plant linked to Salmonella outbreak. The U.S. Food and Drug Administration (FDA) suspended Sunland Inc.'s operations November 26. The New Mexico food producer is linked to Salmonella-tainted peanut butter that has sickened at least 41 people in 2012, the agency said in a statement. The FDA said a review of Sunland Inc.'s product testing records showed that 11 product lots of nut butter tested positive for Salmonella between June 2009 and September 2012. Between March 2010 and September 2012, a portion of eight product lots of nut butter containing Salmonella was distributed by the company to consumers, the organization said. Additionally, the FDA found the presence of Salmonella during its inspection of the plant in September and October, both in samples taken in food production areas and in food products themselves. In a November 15 statement the company said "at no time in its twenty four year history has Sunland, Inc. released for distribution any products that it knew to be potentially contaminated with harmful microorganisms." Source: http://www.reuters.com/article/2012/11/27/usa-salmonella-peanutsidUSL1E8MR00L20121127

Canadian meat processing plant suspended over Listeria scare. Operations were suspended at a meat processing plant in Edmonton, Alberta November 23 after a Listeria infection was detected on an employee, Reuters reported. Capital Packers, Inc., detected the bacteria on an employee and contacted the Canadian Food Inspection Agency (CFIA), which suspended operations at the plant after learning that the company could not properly track the

whereabouts of any of its products. Capital Packers initially told the CFIA that potentially affected products were under its control, but the CFIA determined that products may have been shipped to several provinces. The company sells bacon, sausages, fresh meats, and other products to western Canada and the Northwest Territories. The company has voluntary recalled ham sausages under the brand names Capital and Compliments. Source: http://www.foodsafetynews.com/2012/11/canadian-meat-processing-plant-suspended-over-listeria-scare/

Sunland recall goes international. Peanut products manufactured by Sunland Inc. in Portales, New Mexico, responsible for sickening at least 41 people in the U.S. with Salmonella have fallen under the scrutiny of international food safety authorities in recent weeks, Food Safety News reported November 26. Consumers in Canada, Hong Kong, France, the United Kingdom, Italy, and Norway have received warnings about the potential danger of imported Sunland products. November 21, the UK's Food Standards Agency issued a warning to UK consumers concerning Sunland's products, noting that while Sunland products were likely not sold in UK supermarkets, they may be sold by some online retailers who import American foods. Consumers in Hong Kong were warned of Sunland peanut butter back November 8. Two Sunland-brand Valencia peanut butter products were imported to Hong Kong and may be contaminated. Canadians received a number of warnings about Sunland products as well, with many of the products recalled in the U.S. also having been shipped to Canada. Source: http://www.foodsafetynews.com/2012/11/sunland-recall-goes-international/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+foodsafetynews/mRcs+(Food+Safety+News)

Government Sector (including Schools and Universities)

Egypt clashes cut off access to U.S. Embassy. The U.S. Embassy in Cairo, Egypt, closed November 29 after clashes between opposition protesters and riot police cut off access to the building. The clashes have been ongoing as Egypt's Islamist president refuses to back down in a showdown over decrees granting him near-absolute powers. The protesters do not seem to be targeting the embassy itself; they are targeting the riot police. The clashes are happening in the area and in the approaches to and from the embassy. Most embassy staff have gone home, and the embassy closed for all American citizen services. Source: http://www.cbsnews.com/8301-202_162-57556115/egypt-clashes-cut-off-access-to-u.s-embassy/

(Tennessee) **30 Tenn. courthouses receive bomb threats.** Authorities said 30 Tennessee counties received false bomb threats to courthouses or other government buildings November 27, forcing evacuations while authorities conducted searches. A Tennessee Department of Safety and Homeland Security spokeswoman said no explosives were found and no arrests were made. A spokesman for the Tennessee Emergency Management Agency said the threats were made in phone calls to county clerk offices. In Memphis, police said an unknown woman called and said she had information that someone was going to blow up three buildings in the

city, including the federal building and a post office. Tennessee became the fourth State in November to deal with widespread bomb hoaxes. Oregon, Nebraska, and Washington all had similar threats reported to courthouses. Source: http://www.necn.com/11/27/12/24Tenncourthousesreceivebombthreats/landing_nation.html?&apID=0892ed08ac484c09b1d222334911679c

(Texas) **Anonymous holds school district Web site hostage over student tracking.** Hacktivists associated with the international collective known as Anonymous claimed responsibility for taking down San Antonio, Texas's Northside Independent School District's Web site November 24 in protest of the district's controversial student tracking program. The program requires students to wear name badges that enable school officials to track the location of students. The same hacktivists released another statement November 25 via Pastebin giving the school district "1-3 days" to meet with parents and explain the student tracking program in detail. If the district fails to comply with the request, hacktivists threatened to "simply shut down" the school district Web site once again. Source: http://www.examiner.com/article/anonymous-holds-school-district-website-hostage-over-student-tracking

Information Technology and Telecommunications

Hardcoded account in Samsung printers provides backdoor for attackers. The U.S. Computer Emergency Readiness Team (US-CERT) issued an alert warning users of Samsung printers and some Dell printers manufactured by Samsung about the presence of a hardcoded account that could allow remote attackers to access an affected device with administrative privileges. This privileged access could also be used to change the device configuration, access sensitive information stored on it (credentials, network configuration, etc.), and even to mount additional attacks through arbitrary code execution, US-CERT claims. The hardcoded account is present in all printers released before October 31, 2012. Samsung said that a patch will be pushed out "later this year." Source: http://www.netsecurity.org/secworld.php?id=14020&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Readr

Evolving DDoS attacks force defenders to adapt. In the past, attackers using distributed denial-of-service (DDoS) attacks to take down Web sites or network servers typically adopted one of two tactics; flooding the site with a deluge of data or overwhelming an application server with seemingly valid requests. Yet increasingly, attackers are using a hybrid approach, using multiple vectors to attack. The attacks that hit financial firms in September and October, for example, often used a massive flood of data packets that would overwhelm a victim's network connection, while a much smaller subset of traffic would target vulnerable applications functions, consuming server resources. The one-two punch is potent. Many financial firms thought they had the defenses in place to defeat such attacks but had problems staying accessible during the onslaught. Companies prepared to handle application-layer attacks or smaller volumetric attacks could not handle the 20Gbps or more that saturated their Internet connection. A recent report from network-security firm Prolexic found that the average attack

bandwidth increased to nearly 5Gbps, with 20Gbps attacks quite common. In a year, the average volume of attacks had doubled, the firm found. Source: http://www.darkreading.com/securityservices/167801101/security/perimetersecurity/240142616/evolving-ddos-attacks-force-defenders-to-adapt.html

Symantec warns of new malware targeting SQL databases. Symantec is warning of a new bit of malware that appears to be modifying corporate databases, particularly in the Middle East, though its showing up elsewhere in the world too. W32.Narilam, first discovered November 15, follows a similar pattern of other worms by copying itself onto infected machines, adding registry keys and propagating through removable drives and network shares. "What is unusual about this threat is the fact that it has the functionality to update a Microsoft SQL database if it is accessible by OLEDB. The worm specifically targets SQL databases with three distinct names: alim, maliran, and shahd," wrote a Symantec security researcher. Once Narilam finds the targeted databases, it looks for financial terms such as "BankCheck," "A_sellers" and "buyername" and Persian terms like "Pasandaz" ("Savings") and "Vamghest" ("Instant Loans"). The malware also deletes tables with the following names: A_Sellers, person and Kalamast. "The malware does not have any functionality to steal information from the infected system and appears to be programmed specifically to damage the data held within the targeted database," the researcher wrote. The overall infection rate is low at the moment, but those whose networks are not properly protected could see business disrupted, he said. Source: http://threatpost.com/en_us/blogs/symantec-warns-new-malware-targeting-sql-databases-112312

Researcher finds nearly two dozen SCADA bugs in a few hours' time. A researcher at Exodus Intelligence says that after spending a few hours looking for bugs in SCADA applications, he came up with more than 20, several of which are remote code-execution vulnerabilities. The vice president of research at Exodus said that finding the flaws was not even difficult. In fact, he said that locating the software was more difficult than finding the bugs themselves. He said he decided to go after the SCADA apps, which he had never researched before, after seeing a video posted by ReVuln the week of November 19. In the video, ReVuln researchers say they have server-side remote code-execution flaws in software from GE, Schneider Electric, Siemens, Kaskad, ABB/Rockwell, and Eaton. The Exodus researcher also found flaws in Schneider Electric, Rockwell, and Eaton apps, as well as in software from Indusoft and RealFlex. ReVuln does not disclose vulnerabilities to vendors, but instead keeps the information to itself and sells it to customers. The Exodus researcher, meanwhile, said he plans to disclose all of the bugs he found to the Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT). Of the 23 bugs he discovered, 7 of them were remotely exploitable code execution flaws. Source: http://threatpost.com/en_us/blogs/researcher-finds-nearly-two-dozen-scada-bugs-few-hours-time-112612

National Monuments and Icons

Suspect in string of ecoterrorism fires surrenders. The U.S. attorney's office in Portland, Oregon, reported that a Canadian citizen accused of conspiracy and arson turned herself in to

the FBI at the Canadian border in Blaine, Washington, November 29 after spending years in hiding in Canada. The fugitive was identified as a former wildlife researcher that was part of a cell of the Earth Liberation Front (ELF) and Animal Liberation Front known as The Family, based in Eugene, Oregon. The former wildlife researcher was arrested after spending a decade as an international fugitive from the largest ecoterrorism investigation in U.S. history. She was sought on conspiracy and arson indictments dating to 2006 alleging she helped set fires at the Vail ski resort in Colorado and at federal wild horse corrals in eastern Oregon and northern California, and that she tried to set fire to a lumber mill office in Medford, Oregon. The former wildlife researcher is not specifically charged with terrorism, but the indictment alleges she and the other members of The Family tried to influence businesses and the government and tried to retaliate against the U.S. Forest Service. Authorities said the ELF cell was responsible for 20 arsons around the western U.S. from 1996 to 2001 that caused $40 million in damage. The two remaining fugitives are believed to be in Syria and Europe. Source: http://www.boston.com/business/news/2012/11/29/suspectstringecoterrorismfiressurrenders/qMHiyGRAMlyGEh5y47PYM/story.html

(New York) **Slow, but steady recovery at Staten Island's national parks.** The U.S. National Park Service (NPS) Incident Management Team has been carting off debris, redistributing sand, and assessing damage at its parks and beaches in New York and New Jersey for the past 22 days. On Staten Island, the progress may be most evident at the Gateway National Recreation Area in Great Kills, where commuters boarded the first fast ferries into Manhattan onNovember 26. Th Ranger Station there was reopened and debris removal from the parking lots was 60 percent complete, with sand redistribution at 25 percent complete. At Miller Field in New Drop, debris removal was 60 percent complete and sand redistribution was 40 percent complete. Work continued on water heaters and waterline work. Debris removal at Seabee Park, located at Fort Wadsworth, was 65 percent complete. Both the Statue of Liberty and Ellis Island were to remain closed for the rest of the year. There was no projected opening date for either. Source: http://www.silive.com/news/index.ssf/2012/11/slow_but_steady_recovery_at_st.html

Postal and Shipping

Air freight fire protection unsafe, NTSB says. Fire-protection systems on freight aircraft are inadequate, top U.S. aviation investigators said. The National Transportation Safety Board (NTSB) recommended improvements and rule changes November 28 based on investigations of three catastrophic cargo plane fires. The NTSB chairwoman recommended that the Federal Aviation Administration require better early detection of fires inside cargo containers, development of fire-resistant containers, and requiring active fire-suppression systems on all freight airlines. An NTSB report focused on three cargo fire accidents since 2006. Two of those fires killed the flight crews and destroyed the aircraft. In the third incident, the crew escaped with minor smoke-inhalation difficulties and the plane was significantly damaged. In all three cases, the fires started within the cargo containers aboard the planes, but by the time the plane's fire warning system alerted pilots to the dangers, there was little time for them to react. Federal regulations require cargo airline fire detection systems to alert pilots within a minute of a fire starting, but the NTSB's investigation found current systems detected fire and smoke

anywhere from 2 and one-half minutes to more than 18 minutes after the fires start. The NTSB concluded cargo containers made of flammable materials significantly increase the intensity of the on-board fires because there has been little focus by manufacturers or regulators to develop fire-resistant cargo containers. Additionally, the NTSB's report recommended improved fire suppression systems on cargo planes. Source: http://www.kxly.com/news/Air-freight-fire-protection-unsafe-NTSB-says/-/101270/17583088/-/ygoafv/-/index.html

Public Health

(Washington) **Man charged with donning scrubs, stealing drugs.** A Washington man was charged with donning scrubs and a hospital identification badge to steal drugs from a "crash cart" at a Missoula hospital. Prosecutors said the man left a treatment room in the emergency department November 29, took the scrubs and an ID badge, and was stuffing items from a crash cart into his pockets when an employee saw him. The employee knew the man was not her coworker, led him to an area with more people and whispered to someone to call security. The man fled. He was arrested outside a nearby church. Investigators said he took three syringes, a vial of epinephrine, and two diazepam cartridges.
Source: http://www.sfgate.com/news/crime/article/Man-charged-with-donning-scrubsstealing-drugs-4080390.php

Pacemakers, other implanted devices, vulnerable to lethal attacks. IT experts reported security flaws in pacemakers and defibrillators could be putting lives at risk, stating that many devices are not properly secured and therefore are vulnerable to hackers who may want to commit an act that could lead to multiple deaths, Homeland Security reported November 28. The Sydney Morning Herald reported that a famous hacker hacked into a pacemaker in October at the Breakpoint security conference in Melbourne, Australia, and was able to deliver an 830-volt jolt to a pacemaker by logging into it remotely after hacking the device. He, however, did not reveal which models were vulnerable to hackers. The hack was possible because many implanted medical devices use wireless technology and authentication which uses a name and a password, which is the serial and model number of the device. According to the hacker, most medical devices are designed to be easy to access by a doctor who may need to change something quickly in case of an emergency. The hacker found secret commands that doctors use in order to send a "raw packet" of data over the airwaves to find any pacemaker or defibrillator in a specific range and have it respond with its serial and model number. The information allows a hacker to authenticate a device to receive data and perform commands, meaning they can send a command to jolt the heart of multiple devices and, in some cases, in a range of up to twelve meters. The U.S.Government Accountability Office released a report that highlighted problems with the security of medical devices, and called upon the Food and Drug Administration to ensure devices are secure from these attacks. Source: http://www.homelandsecuritynewswire.com/dr20121128pacemakers-otherimplanted-devices-vulnerable-to-lethal-attacks

Transportation

Drought threatens to close Mississippito barges. If water levels fall too low, the nation's main inland waterway, the Mississippi River, could become impassable to barges just as the harvest heads to market, the Associated Press reported November 29. Shipping companies are scrambling to find alternative ways to move tons of corn, wheat and other crops to the Gulf Coast for shipment overseas. The Mississippi River is approaching the point where it may become too shallow for barges that carry food, fuel, and other commodities. If the river is closed for a lengthy period, experts say, economic losses could climb into the billions of dollars. The focus of greatest concern is a 180-mile stretch of the river between the confluences of the Missouri River near St. Louis and the Ohio River at Cairo, Illinois. That is where lack of rain has squeezed the channel from its normal width of 1,000 feet or more to just a few hundred feet. The river depth is 15 to 20 feet less than normal, now about 13 feet deep in many places. If it dips to around 9 feet, rock pinnacles at two locations make it difficult, if not impossible, for barges to pass. Hydrologists for the National Weather Service predict the Mississippi will reach the 9-foot mark by December 9. The week of November 19, the Army Corps of Engineers began reducing the outflow from an upper Missouri River dam in South Dakota, where a group of experts said November 30 that the worst U.S. drought in decades had intensified. A two-month shutdown — the length of time that some observers fear given current conditions — would have an estimated impact of $7 billion, according to the river industry trade group American Waterways Operators. Source: http://www.vcstar.com/news/2012/nov/29/drought-threatens-toclosemississippitobarges/

More fraudulent letters sent to motor carriers. Another round of fraudulent U.S. Department of Transportation (U.S. DOT) letters dated September 24, 2012 were being distributed — largely by fax — to motor carrier officials attempting to obtain banking information from the targeted carriers, according to the Federal Motor Carrier Safety Administration (FMCSA), Fleet Owner reported November 28. The letters appear to be from the "U.S. Department of Transportation Procurement Office" and are signed by a fictitious name. The individual on the letter is not an employee of U.S. DOT, FMCSA said. This was one of manyrounds of the scam where many carriers have received a faxed letter asking recipients to provide bank account information on an "Authorization to Release Financial Information" form. In the recurring identity theft scheme the letters are typically signed by someone claiming to be a "Senior Procurement Officer" at DOT and appear on DOT letterhead containing a Washington, D.C. address.
Source: http://fleetowner.com/fleet-management/more-fraudulent-letters-sent-motorcarriers

Water and Dams

Nothing Significant to Report

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168